

CTO 15431 US / swg

日 本 国 特 許
JAPAN PATENT OFFICE



09/867,470
GM4:2151

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 5月11日

RECEIVED

SEP 10 2001

出 願 番 号

Application Number:

特願2001-141774

Technology Center 2100

出 願 人

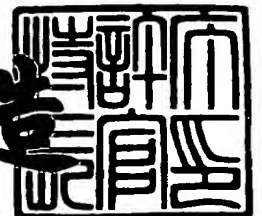
Applicant(s):

キヤノン株式会社

2001年 6月26日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3060224

【書類名】 特許願

【整理番号】 4462021

【提出日】 平成13年 5月11日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 1/00

【発明の名称】 ネットワークシステム、W e bサーバへのアクセス制限
方法、記憶媒体、ネットワークデバイス及びその制御方
法、並びにプログラム

【請求項の数】 14

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会
社内

【氏名】 横倉 秀則

【特許出願人】

【識別番号】 000001007

【氏名又は名称】 キヤノン株式会社

【代表者】 御手洗 富士夫

【代理人】

【識別番号】 100081880

【弁理士】

【氏名又は名称】 渡部 敏彦

【電話番号】 03(3580)8464

【先の出願に基づく優先権主張】

【出願番号】 特願2000-176128

【出願日】 平成12年 6月12日

【手数料の表示】

【予納台帳番号】 007065

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9703713

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークシステム、Webサーバへのアクセス制限方法、記憶媒体、ネットワークデバイス及びその制御方法、並びにプログラム

【特許請求の範囲】

【請求項1】 複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの1つがWebクライアントを搭載しており、前記コンピュータの他の1つ及び前記ネットワークデバイスの1つの一方がWebサーバを搭載しているネットワークシステムにおいて、前記Webサーバは、前記Webサーバへのアクセスを制限することを決定する決定手段と、前記Webサーバへのアクセスを制限することが決定されたときに、前記Webサーバへのアクセスが制限されていることを示すデータを前記Webクライアントに通知する通知手段とを備えることを特徴とするネットワークシステム。

【請求項2】 前記通知手段は、前記Webサーバへのアクセスを制限することが決定されたとき、且つ前記Webクライアントが前記データの更新日付を指定したときに、当該更新日付以降に前記データが更新されているか否かに拘わらず、前記Webサーバへのアクセスが制限されていることを示すデータを前記Webクライアントに通知することを特徴とする請求項1記載のネットワークシステム。

【請求項3】 前記Webサーバは、前記ネットワークデバイスの1つに搭載されていることを特徴とする請求項2記載のネットワークシステム。

【請求項4】 前記Webサーバは、前記コンピュータの他の1つに搭載され、且つ、前記複数のネットワークデバイスの状況を前記Webクライアントに通知する他の通知手段を備えることを特徴とする請求項2記載のネットワークシステム。

【請求項5】 複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの1つがWebクライアントを搭載しており、前記コンピュータの他の1つ及び前記ネットワークデバイスの1つの一方がWebサーバを搭載しているネットワークシステムにおける

W e bサーバへのアクセス制限方法において、前記W e bサーバへのアクセスを制限することを決定する決定工程と、前記W e bサーバへのアクセスを制限することが決定されたときに、前記W e bサーバへのアクセスが制限されていることを示すデータを前記W e bクライアントに通知する通知工程とを備えることを特徴とするW e bサーバへのアクセス制限方法。

【請求項6】 前記通知工程は、前記W e bサーバへのアクセスを制限することが決定されてたとき、且つ前記W e bクライアントが前記データの更新日付を指定したときに、当該更新日付以降に前記データが更新されているか否かに拘わらず、前記W e bサーバへのアクセスが制限されていることを示すデータを前記W e bクライアントに通知することを特徴とする請求項5記載のW e bサーバへのアクセス制限方法。

【請求項7】 前記W e bサーバは、前記ネットワークデバイスの1つに搭載されていることを特徴とする請求項6記載のW e bサーバへのアクセス制限方法。

【請求項8】 前記W e bサーバは、前記コンピュータの他の1つに搭載され、且つ、前記複数のネットワークデバイスの状況を前記W e bクライアントに通知する他の通知工程を備えることを特徴とする請求項6記載のW e bサーバへのアクセス制限方法。

【請求項9】 複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの1つがW e bクライアントを搭載しており、前記コンピュータの他の1つ及び前記ネットワークデバイスの1つの一方がW e bサーバを搭載しているネットワークシステムにおけるW e bサーバへのアクセス制限方法を実行するプログラムを記憶した読み出し可能な記憶媒体であって、前記W e bサーバへのアクセス制限方法は、前記W e bサーバへのアクセスを制限することを決定する決定工程と、前記W e bサーバへのアクセスを制限することが決定されたときは、前記W e bサーバへのアクセスが制限されていることを示すデータを前記W e bクライアントに通知する通知工程とを備えることを特徴とする記憶媒体。

【請求項10】 ネットワークに接続されたネットワークデバイスにおいて

、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別手段と、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信手段とを備えることを特徴とするネットワークデバイス。

【請求項 1 1】 更に、前記他のネットワークデバイスからの日時情報を検出する検出手段を備え、前記送信手段は、前記他のネットワークデバイスからのアクセスを制限しないときは、前記検出された日時情報に応じて前記ネットワークデバイスのステータスを示す情報を前記他のネットワークデバイスに送信することを特徴とする請求項 1 0 記載のネットワークデバイス。

【請求項 1 2】 更に、前記他のネットワークデバイスからの日時情報を検出する検出手段を備え、前記送信手段は、前記他のネットワークデバイスからのアクセスを制限するときは、前記検出された日時情報に拘わらず前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信することを特徴とする請求項 1 0 記載のネットワークデバイス。

【請求項 1 3】 ネットワークに接続されたネットワークデバイスの制御方法において、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別工程と、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信工程とを備えることを特徴とするネットワークデバイスの制御方法。

【請求項 1 4】 ネットワークに接続されたネットワークデバイスの制御方法を実行するプログラムにおいて、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別ステップと、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信ステップとを含むことを特徴とするプログラム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ネットワークシステム、Webサーバへのアクセス制限方法、記憶媒体、ネットワークデバイス及びその制御方法、並びにプログラムに関する。

【0002】

【従来の技術】

近年、複数のコンピュータや複数のプリンタ等のネットワークデバイスが接続されたネットワークを介して行われるインターネットが急速に普及し、このインターネットを利用した様々なアプリケーションが開発されている。将来的には、このインターネット利用技術は急速に進むことが予想されている。その中で、ネットワークに接続されるプリンタ等のネットワークデバイスにWebサーバの機能を搭載することにより、ネットワークデバイスにアクセスして、ネットワークデバイスのステータスや印刷ジョブ等を市販のWebブラウザを用いて参照することができる製品が開発されている。このようなネットワークデバイスでは、その初期設定値等がデバイス管理者により設定されている。デバイス管理者は、ネットワークデバイスのメンテナンス中などに設定がユーザによって書き換えられるのを防止するためにWebサーバへのアクセスを制限する手立てを講じる必要がある。

【0003】

【発明が解決しようとする課題】

しかしながら、Webサーバへのアクセスを制限し、アクセスが禁止されているユーザからのアクセスを受けた場合に、403 Forbidden等のエラーコードを該ユーザに送信することでアクセスが制限されていることを通知することも可能であるが、このエラーコードでは情報量が乏しいため、Webサーバへのアクセスを制限した理由がユーザに明確に通知することができない。

【0004】

また、HTMLファイルを動的に変更することによりWebサーバへのアクセスが制限されている旨を通知することも可能であるが、Webサーバへアクセスしたときは、HTMLファイルの更新日付指定の如何に拘わらず、ユーザ側のWebブラウザでキャッシュしていたHTMLファイルを表示してしまい、更新日

付以降にHTMLファイルが更新されていた場合であっても、表示データの量を低減することができない。

【0005】

本発明の目的は、ネットワークデバイスへの最新のアクセス制限の理由を明確、且つ確実にユーザに通知することができ、また、ユーザに通知する表示用データの量を低減することにある。

【0006】

【課題を解決するための手段】

上記目的を達成するために、ネットワークシステムは、複数のコンピュータ及び複数のネットワークデバイスが接続されたネットワークシステムであって、前記コンピュータの1つがWebクライアントを搭載しており、前記コンピュータの他の1つ及び前記ネットワークデバイスの1つの一方がWebサーバを搭載しているネットワークシステムにおいて、前記Webサーバは、前記Webサーバへのアクセスを制限することを決定する決定手段と、前記Webサーバへのアクセスを制限することが決定されたときに、前記Webサーバへのアクセスが制限されていることを示すデータを前記Webクライアントに通知する通知手段とを備えることを特徴とする。また、そこで使われるWebサーバへのアクセス制限方法、該アクセス制限方法を実行するプログラムを記憶した記憶媒体を提供する。

【0007】

上記目的を達成するために、ネットワークデバイスは、ネットワークに接続されたネットワークデバイスにおいて、前記ネットワークに接続された他のネットワークデバイスからのアクセスを制限するか否かを判別する判別手段と、前記他のネットワークデバイスからのアクセスを制限するときは、前記アクセスを制限している理由を示す情報を前記他のネットワークデバイスに送信する送信手段とを備えることを特徴とする。また、その制御方法、該制御方法を実行するプログラムを提供する。

【0008】

【発明の実施の形態】

以下、本発明の実施の形態に係るネットワークシステムを図面を参照して説明する。

【0009】

図1は、本発明の実施の形態に係るネットワークシステムの構成図である。

【0010】

図1において、LAN100（ネットワーク）には、カラープリンタ101、ネットワークプリンタとして使用可能なコピー機等のMFP（Multi Function Peripheral）102、モノクロプリンタ103、ファクシミリ104、及びスキャナ105、106から成る複数のネットワークデバイスと、デスクトップPC111、112及びノートPC113から成る複数のコンピュータとが接続されている。カラープリンタ101、MFP102、モノクロプリンタ103、ファクシミリ104、及びデスクトップPC111、112は、ビルの2階に配されており、スキャナ105、106及びノートPC113は、ビルの1階に配されている。ノートPC113は、ポータブルであるので、LAN100から外されることもあり得る。

【0011】

デスクトップPC111、112及びノートPC113には、夫々、Webサーバ機能を搭載したネットワークデバイスのステータス（状況）等を参照するWebブラウザが搭載されており、これらのPCは、ネットワークデバイス間でHTML（Hypertext Markup Language）文書を送受信するためのHTTP（Hypertext Transfer Protocol）によるアクセスが可能である。

【0012】

上記ネットワークデバイスの少なくとも1つには、Webサーバ（Webサーバ機能）が搭載されており、コンピュータの少なくとも1つには、Webクライアント（Webクライアント機能）が搭載されている。

【0013】

更に、ネットワーク100は、ファイアウォール120を介してインターネット130に接続されており、インターネット130を介して他のネットワーク140とも接続されている。

【 0 0 1 4 】

図 2 は、図 1 のネットワークシステムにおけるネットワークデバイスの内部構成のブロック図である。

【 0 0 1 5 】

図 2 において、Webサーバ機能を搭載するネットワークデバイスは、制御部 2 0 0、周辺機器制御部 2 0 1、及びLANプロトコル制御部 2 0 2 を有しており、これらは、各制御部を総括的に制御する制御バス 2 0 3 に夫々接続されていると共に、データバス 2 0 4 にも夫々接続されている。データバス 2 0 4 には、プリンタやファクシミリ等の周辺機器が接続されている。また、制御部 2 0 0 は、CPU、ROM、RAM、バックアップRAM等で構成されている。例えば、CPUは、ROMに格納されているプログラムに従ってネットワークデバイスがメンテナンス中か否かを判別し、メンテナンス中である場合はアクセス制限を行うと判断する。なお、バックアップRAMには、CPUがアクセス制限するか否かを判断するためのフラグが格納されている。周辺機器制御部 2 0 1 は、データバス 2 0 4 を介してプリンタやファクシミリ等の周辺機器にデータを送受信する。LANプロトコル制御部 2 0 2 には、LAN 1 0 0 を介して他のネットワーク機器又は他のPCと双方向にデータを送受信する。

【 0 0 1 6 】

図 3 は、本発明の実施の形態に係るネットワークシステムが実行するWebサーバ機能を搭載したネットワークデバイスへのアクセス制限処理のフローチャートである。

【 0 0 1 7 】

図 3 において、Webサーバ機能を搭載するネットワークデバイス（以下「Webサーバ」という。）の起動後に、Webクライアント機能を搭載するコンピュータ（以下「Webクライアント」という。）からWebサーバへのアクセスがなされると（ステップ S 3 0 0 で YES）、WebサーバはWebサーバ本体の格納手段に格納されているアクセス制限情報の参照を行い（ステップ S 3 0 1）、Webクライアントからのアクセスを制限するか否かを判別する（ステップ S 3 0 2）（判別・決定手段）。上記アクセス制限情報は、ネットワークデバイス

のデバイス管理者が設定した、当該ネットワークデバイスのWebサーバへのアクセス制限を判断するための情報である。

【 0 0 1 8 】

ステップS302の判別の結果、アクセス制限情報によりWebクライアントからのアクセスを制限しないときは（アクセスを許可するとき）、ステップS303に進んで、Webクライアントから「If-Modified-Since」要求があるか否かを判別する。ここで、「If-Modified-Since」要求とは、Webクライアントから送出される日付（日時）情報付きの要求であって、その日付（日時）以降にWebサーバのHTMLファイルが更新されていなければ、HTMLファイル更新されていないことを示す「Not Modified」を送信することにより、ネットワークの受信負荷を削減するためのものである。また、Webクライアントは、ユーザの指定したURLに相当するファイルを既にキャッシュしている場合に、この「If-Modified-Since」要求を送出する。

【 0 0 1 9 】

ステップS303の判別の結果、Webクライアントから「If-Modified-Since」要求があるときは、ステップS304に進んで、「If-Modified-Since」に付加されてきた日付（日時）情報を検出し（検出手段）、該日時情報を用いてWebクライアントが保持しているHTMLファイルの日時情報と比較して、Webサーバが保持しているHTMLファイルが更新されているか否かを判別する（ステップS304）。ステップS304の判別の結果、Webクライアントが通知してきた日付（日時）以降にファイルが更新されていないときは、HTMLファイルの変更がされていないことを示す「Not Modified」をWebクライアントに送信する（ステップS305）。一方、HTMLファイルが更新されているときは、後述する図5（a）に対応するHTMLファイルのデータ（デバイス情報）を更新したファイルとしてWebクライアントに送信して（ステップS306）、本処理を終了する。ステップS306では、特に指定されていなければ、ネットワークデバイスで特定されているTopページのHTMLファイルを送信する。

【 0 0 2 0 】

ステップ S 3 0 3 の判別の結果、W e b クライアントから「If-Modified-Since」要求がないときは、HTML ファイルが更新されているか否かに拘わらず、後述する図 5 (a) に対応する HTML ファイルのデータ (デバイス情報) を W e b クライアントに送信して (ステップ S 3 0 6) 、本処理を終了する。

【 0 0 2 1 】

ステップ S 3 0 2 の判別の結果、アクセス制限情報により W e b クライアントからのアクセスを制限するときは (アクセスを許可しないとき) 、ステップ S 3 0 7 に進んで、W e b クラアントから「If-Modified-Since」要求があるか否かを判別し、「If-Modified-Since」要求がないときは、予め用意しておいた W e b サーバへのアクセス制限及びその理由を示す情報、すなわち後述する図 5 (b) に対応する HTML ファイル (図 5 (b)) のデータ (デバイス情報) を W e b クライアントに送信することにより、アクセスが制限されていることをユーザに通知して (ステップ S 3 0 8) (通知・送信手段) 、本処理を終了する。一方、ステップ S 3 0 7 の判別の結果、「If-Modified-Since」要求があるときは、W e b クライアントが保持している HTML ファイルの日時以降に W e b サーバが保持している HTML ファイルが更新されているか否かの判別を行うことなく (ステップ S 3 0 9) 、上記ステップ S 3 0 8 の処理を実行して、本処理を終了する。

【 0 0 2 2 】

図 4 は、W e b クライアント及び W e b サーバ間の HTTP シーケンスの一例を示す図である。以下の説明では、図 3 のフローチャートにおけるステップ番号の付記により、図 3 の説明と対応させている。

【 0 0 2 3 】

図 4 において、カラープリンタ 1 0 1、MFP 1 0 2、モノクロプリンタ 1 0 3、及びファクシミリ 1 0 4 等のネットワークデバイスの少なくとも 1 つには、W e b サーバ 4 0 1 が搭載されている。また、デスクトップ PC 1 1 1、1 1 2 及びノート PC 1 1 3 の少なくとも 1 つには、W e b クライアント 4 0 0 が搭載されている。

【 0 0 2 4 】

まず、Webクライアント400に、デスクトップPC111、112及びノートPC113等に搭載されているWebブラウザからパケットが送信され、そのWebブラウザのURLで特定のWebサーバ401を指定したときに、そのWebサーバ401のTopページの情報をWebクライアント400が保持していたならば、Webクライアント400は、データ取得要求としてGET / HTTP/1.0 If-Modified-Since: Tuesday, 30-Feb-00... により、Webサーバ401へのアクセスの制限がなされているか否かの問い合わせを開始する(402)(図3のステップS300)。

【0025】

次いで、Webサーバ401は、GET Ackを返信することにより、Webクライアント400に対して、データを確実に取得したことを通知する(403)と共に、データ取得要求(402)に対するWebサーバ401のステータスを検出された日時情報に応じて返信する(404)(図3のステップS302、S307)。ここでは、正常なステータスを示す情報であるHTTP/1.0 200 OKを返信し、その後、<html>.<head>... __err.gif...により、Webサーバ401へのアクセスが制限されていることを示すHTMLファイルを返信する(405)(図3のステップS308)。ここでは、HTMLファイルが画像データファイル__err.gifを含んでいるので、Webクライアント400は、GET /__err.gif HTTP/1.0 ... により、画像データファイル__err.gifの取得を要求し(406)、Webサーバ401は、その要求に対する応答として後述する図5(b)に対応するHTMLファイルをWebクライアント400に対して送信する(407)。

【0026】

図5は、Webサーバへアクセスした場合のWebブラウザの表示例を示す図であり、(a)は一般的なWebブラウザの場合、(b)はWebサーバへのアクセスが制限されている場合である。

【0027】

まず、図5(a)において、Webブラウザ500は、一般的なWebブラウザの画面502を示しており、IPアドレスを指定してネットワークデバイスを特定するURL501を含む。本例では、プリンタの画像と、このステータスが

表示されている。なお、ファイル名を特に指定しない場合には、Webサーバ401が保持しているTopページのデータを表示する。

【0028】

一方、図5（b）において、Webブラウザ503は、デバイス管理者が、Webサーバ401へのアクセスを制限している場合にWebサーバ401から送信される画面505を示している。画面505上の画像データや文字データにより、Webサーバ401へのアクセスが制限された状態であることをWebクライアント400に明確に通知することができる。

【0029】

Webブラウザ500、503としては、代表的なものとしては、マイクロソフト社のInternet Explorerや、ネットスケープ社のNetscape Communicator等が挙げられる。

【0030】

本実施の形態によれば、Webサーバへのアクセスを制限することが決定しているときに（ステップS302でYES）、Webサーバへのアクセスが制限されていること、及びその理由を示すHTMLファイル（図5（b））のデータをWebクライアントに通知する（ステップS308）ので、Webクライアントに通知されたHTMLファイルによって、Webサーバへのアクセス制限及びその理由（メンテナンス中など）をユーザに確実に通知することができる。また、Webサーバへのアクセスを制限することが決定しているとき（ステップS302でYES）、且つWebクライアントがデータの更新日付を指定しているときに（ステップS307でYES）、HTMLファイルの更新日時比較を行うことなく（ステップS309）、Webサーバへのアクセスが制限されていること、及び、その理由を示すHTMLファイル（図5（b））をWebクライアントに通知する（ステップS308）ので、WebブラウザでキャッシュしていたHTMLファイルを表示するのを防止でき、確実に最新の理由等を通知することができる。また、アクセス制限がされていない場合は、検出された日時情報（更新日時）に応じてWebサーバのステータスを示す情報をWebクライアントに送信するので、表示データの量を低減することができる。

【 0 0 3 1 】

なお、上記実施の形態において、デバイス情報の通知をHTMLファイルにより行っているが、テキストファイルや画像ファイル等によって行ってもよい。また、上記実施の形態において、Webサーバ機能がネットワークデバイスに搭載されているが、Webサーバ機能がコンピュータに搭載されて、プロキシサーバの役割を担うことにより、デバイス情報をWebクライアントに送信してもよい。また、Webクライアント機能を搭載したネットワークデバイスと、Webサーバ機能を搭載したネットワークデバイスとの間で上記図3の処理及び図4のシーケンスを行ってもよい。

【 0 0 3 2 】

上記実施の形態では、Webサーバへのアクセス制限処理を説明したが、この処理をプログラムとして書き込み、装置で該記憶媒体から上記プログラムを読み出して実行しても、上述した処理を実行することができる。また、記憶媒体は、フロッピー（登録商標）ディスク、ハードディスク、CD-ROM、MO等の様々なものが考えられるが、特定のものに限定する必要はなく、上記プログラムを記憶できるものであればよい。

【 0 0 3 3 】

【発明の効果】

以上詳細に説明したように、本発明によれば、Webサーバ等のネットワークデバイスへの最新のアクセス制限の理由を明確、且つ確実にユーザに通知することができ、また、ユーザに通知する表示用データの量を低減することができる。

【 0 0 3 4 】

例えば、アクセスを制限する場合は、WebブラウザでキャッシュしていたHTMLファイルを表示するのを確実に防止することができる。さらに、WebブラウザでキャッシュしているHTMLファイルの日時情報に応じて、該HTMLファイルを表示させるので、ユーザに通知する表示用データの量を低減することができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態に係るネットワークシステムの構成図である。

【図 2】

図 1 のネットワークシステムにおけるネットワークデバイスの内部構成のブロック図である。

【図 3】

本発明の実施の形態に係るネットワークシステムが実行する Web サーバ機能を搭載したネットワークデバイスへのアクセス制限処理のフローチャートである。

【図 4】

Web クライアント及び Web サーバ間の HTTP シーケンスの一例を示す図である。

【図 5】

Web サーバへアクセスした場合の Web ブラウザの表示例を示す図であり、(a) は一般的な Web ブラウザの場合、(b) は Web サーバへのアクセスが制限されている場合である。

【符号の説明】

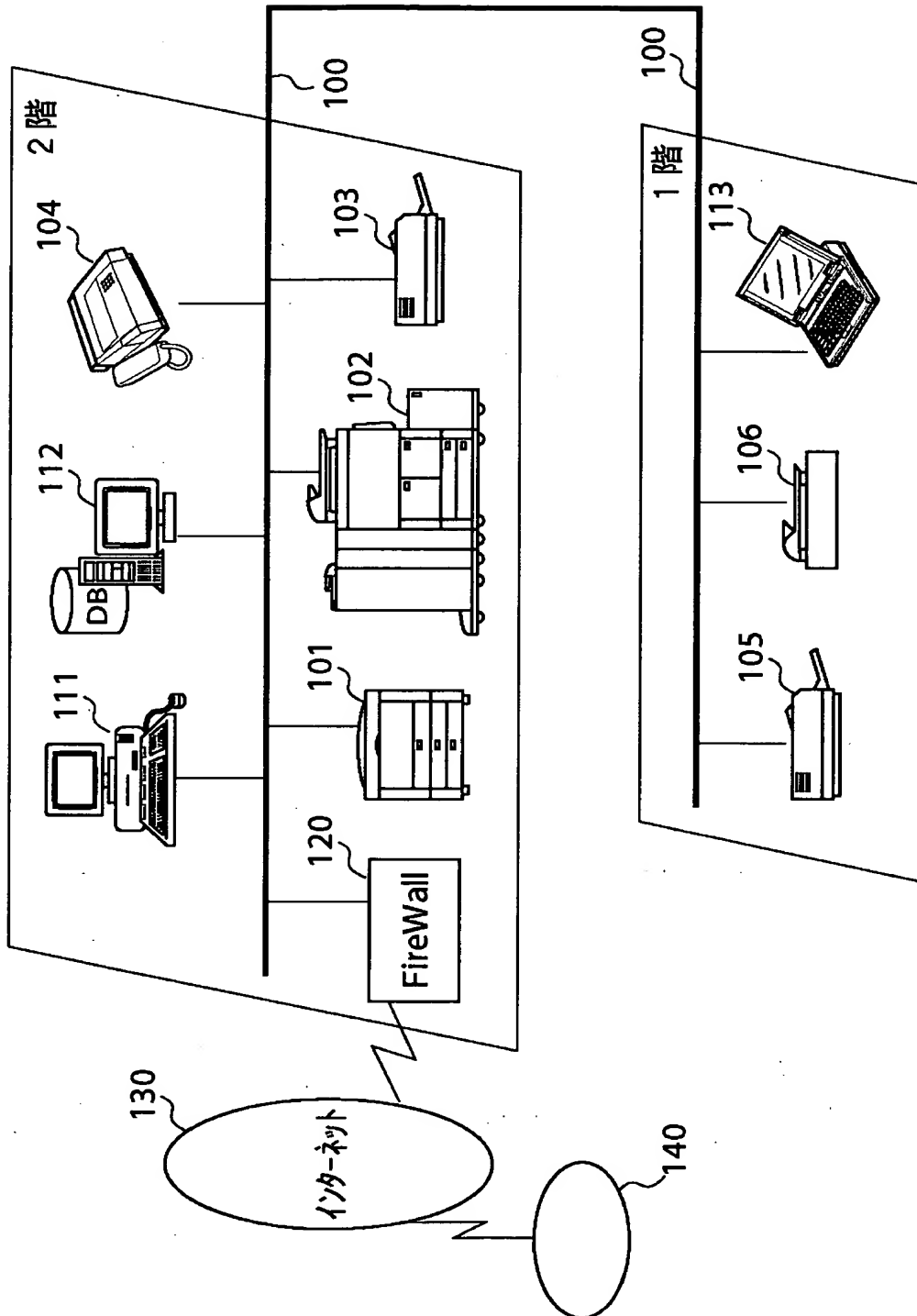
1 0 0, 2 0 5 LAN
1 0 1 カラープリンタ
1 0 2 MFP
1 0 3 モノクロプリンタ
1 0 4 ファクシミリ
1 0 5, 1 0 6 スキャナ
1 1 1, 1 1 2 デスクトップ PC
1 0 3 ノート PC
1 3 0 インターネット
1 4 0 他のネットワーク
2 0 0 制御部
2 0 1 周辺機器制御部
2 0 2 LAN プロトコル制御部

2 0 3 制御バス

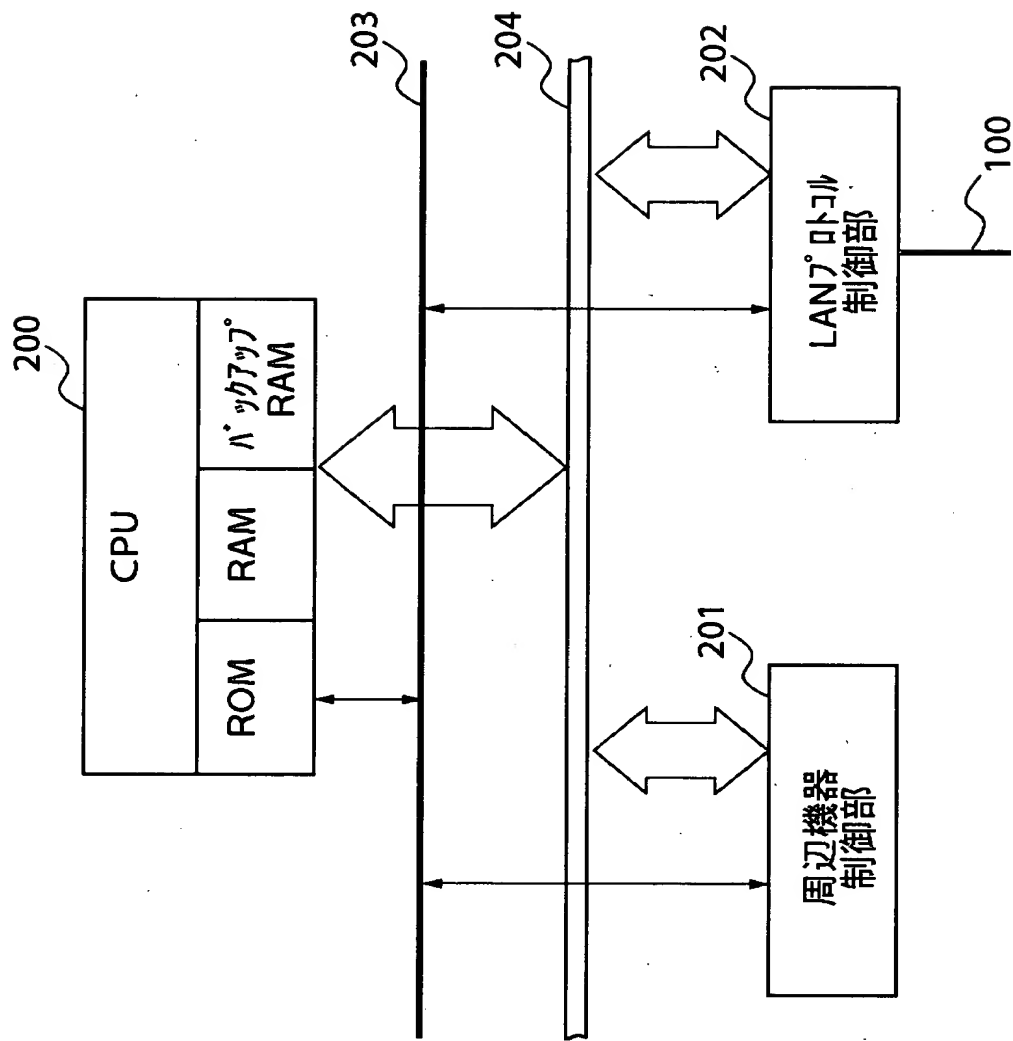
2 0 4 データバス

【書類名】 図面

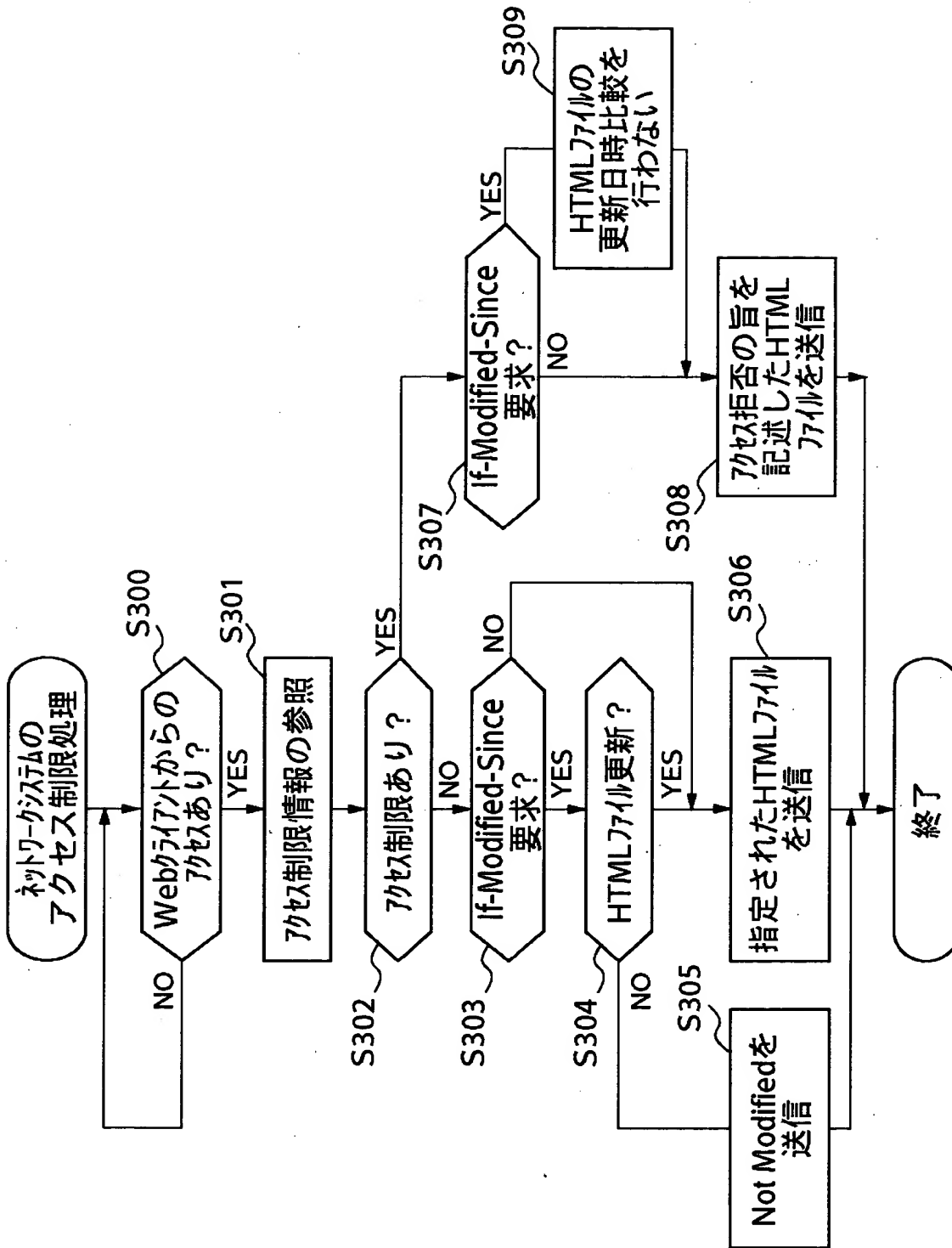
【図 1】



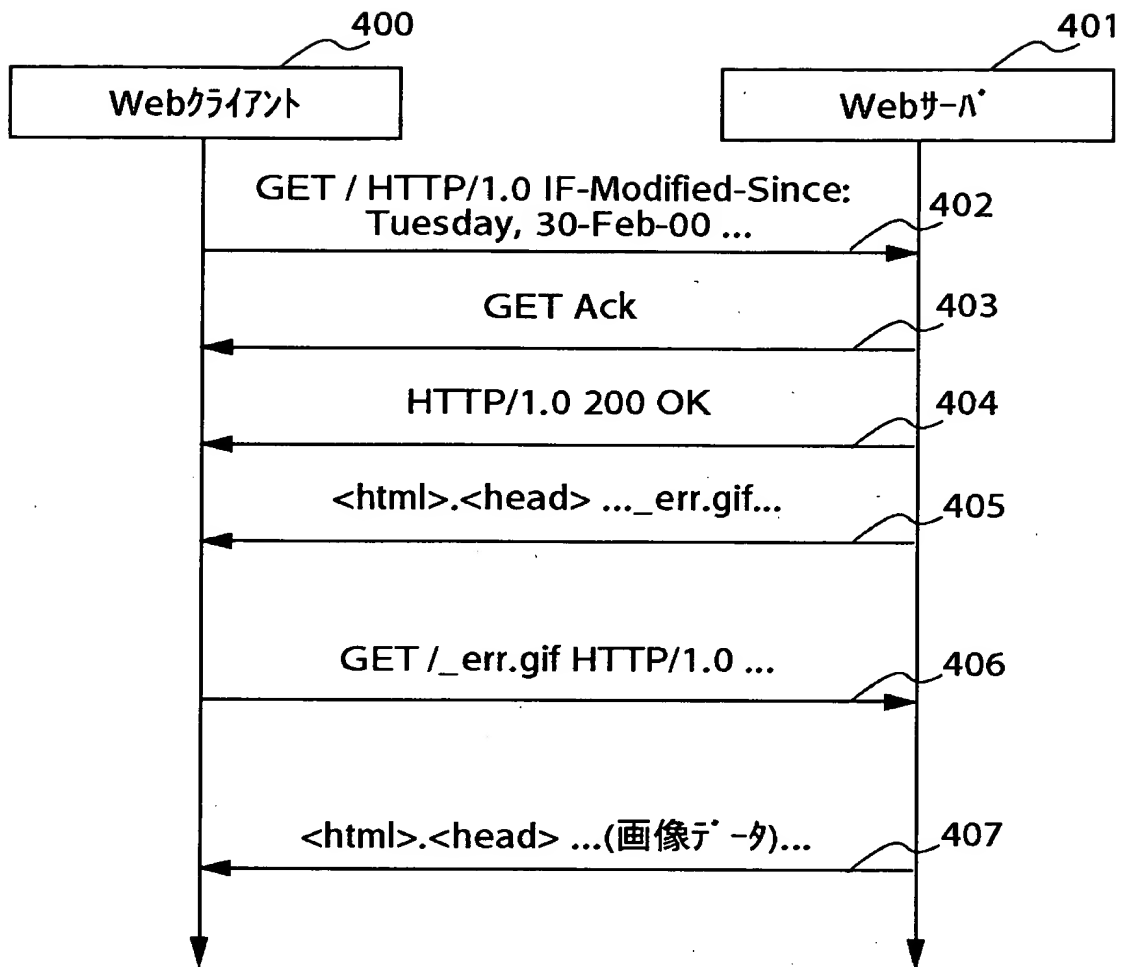
【図 2】



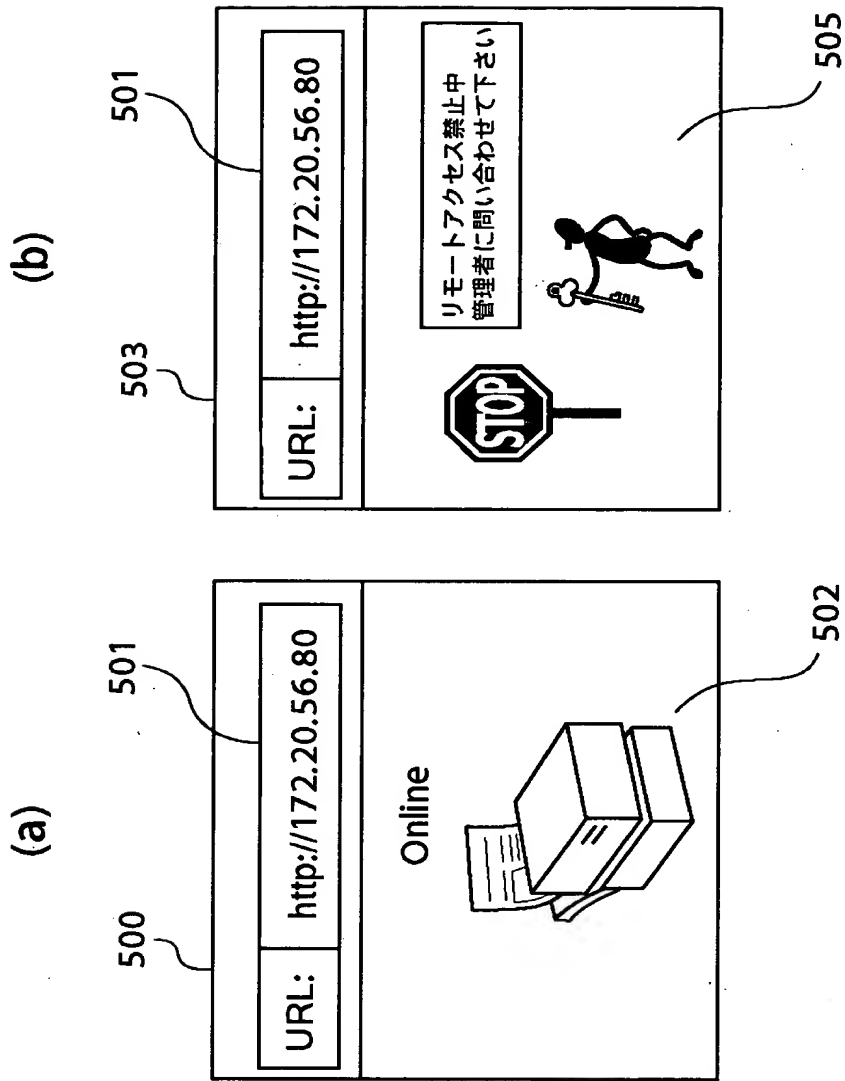
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 ネットワークデバイスへの最新のアクセス制限の理由を明確、且つ確実にユーザに通知することができ、更にユーザに通知する表示用データの量を低減することができるネットワークシステム、Webサーバへのアクセス制限方法、記憶媒体、ネットワークデバイス及びその制御方法、並びにプログラムを提供する。

【解決手段】 LAN100には、複数のネットワークデバイスと、複数のコンピュータとが接続されている。ネットワークデバイスの少なくとも1つには、Webサーバ機能が搭載されており、コンピュータの少なくとも1つには、Webクライアントが搭載されている。Webサーバへのアクセスを制限することが決定しているときには、Webサーバへのアクセスが制限されていることを示すHTMLファイル（図5（b））をWebクライアントに通知する。Webクライアントは通知されたHTMLファイルによって、Webサーバへのアクセス制限及びその理由等をユーザに確実に通知することができる。

【選択図】 図3

5

認定・付加情報

特許出願の番号	特願2001-141774
受付番号	50100684410
書類名	特許願
担当官	第三担当上席 0092
作成日	平成13年 5月25日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子3丁目30番2号
【氏名又は名称】	キャノン株式会社

【代理人】

申請人	
【識別番号】	100081880
【住所又は居所】	東京都港区虎ノ門1丁目17番1号 虎ノ門5森ビル 渡部国際特許事務所
【氏名又は名称】	渡部 敏彦

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都大田区下丸子3丁目30番2号
氏 名 キヤノン株式会社